DOMAIN NAME BLOCKCHAIN USER ADDRESSES

FIELD

This disclosure relates generally to blockchains, and, more particularly, blockchain user addresses.

BACKGROUND

The domain name system (DNS) is a hierarchical distributed naming system for resources provided by computer servers that are connected to the internet. It associates domain names to numeric internet protocol (IP) addresses of internet resources. The DNS thus allows computers and humans to access networked resources, including web pages, using domain names.

Domain names have levels, e.g., for example.com, the "com" portion is referred to as the "top-level domain name", and the "example" portion is referred to as the "second-level domain name". This convention may be continued indefinitely, e.g., for the domain name sub.example.com, the "sub" portion is referred to as a "third-level domain name". As used herein, unless otherwise qualified by specifying the level, the term "domain name" means full domain name, including a top-level domain name, a second-level domain name, and possibly additional levels of domain names.

A DNS "registry" is an authoritative, master database of all domain names registered in a top-level domain or other domain in which domain names can be registered. A registry includes many hardware computer servers operably coupled to the internet. For ease of discussion, a registry is identified with its hardware computer servers unless otherwise specified or clear from context. Internet users generally interact with the registry via intermediaries such as registrars.

"Registrars" are companies that register ownership of domain names by entities known as "registrants". Registrars compete with one another to register domain names for registrants through the registry. That is, an internet user interacts with a registrar to obtain ownership of a domain name, thereby becoming a registrant for the domain. Registrars typically include many hardware computer servers. For ease of discussion, a registrar is identified with its hardware computer servers unless otherwise specified or clear from context. Further, for ease of discussion, a registrant is identified with its hardware client computer unless otherwise specified or clear from context.

Trusted "service providers" provide DNS-related services but are not official DNS registries or other official DNS entities. For example, web hosting providers provide the web server computers that serve the web pages associated with domain names. These entities are trusted service providers in the DNS context. As another example, consumer DNS resolvers provide DNS resolution services separate from the official distributed database of DNS data maintained by the official DNS registries. Such DNS operators are also a type of trusted service provider. As yet another example, trusted service providers in the DNS context may act on a user's behalf, e.g., to enable DNSSEC for a registrant's domain. Other trusted service providers exist.

A "blockchain" is a decentralized, distributed, electronic ledger that records transactions, including but not limited to cryptocurrency transactions, or other information, as described presently. In general, a blockchain takes the form of a distributed readable and writeable computer interpretable data structure, stored in various computers (i.e., nodes) in the blockchain network (e.g., a cryptocurrency network). A blockchain is constructed from individual logical blocks. Each block may include any, or a combination, of: a timestamp representing a time of the block's creation, a cryptographic hash of an identification of the previous block, and a payload, which includes data that may represent transactions or other information. The data in the blockchain payload may represent, for example, for each of a plurality of transactions, a transaction identifier, a transaction amount, and the address associated with the receiving party (more precisely, associated with the receiving party's public key). Each participant in the blockchain network is associated with a cryptographic asymmetric key pair, referred to as the participant's "blockchain key pair", consisting of a public key (e.g., usable by the participant to receive cryptocurrency) and a private key (e.g., usable by the participant to send cryptocurrency). In particular, the public key is associated with (e.g., usable to derive via cryptographic hash) a "blockchain user address" of the participant, and the private key is owned or controlled—and kept secret—by the blockchain network participant. A first blockchain participant may receive cryptocurrency from a second blockchain participant, for example, that utilizes a cryptocurrency blockchain user address of the first blockchain participant. For brevity, blockchain user addresses are referred to as "addresses" herein when clear from context.

SUMMARY

According to various embodiments, a domain name system (DNS) registry facilitated method of assigning a DNS domain name registered to a registrant as a blockchain user address in a blockchain network is disclosed. The method includes: obtaining, by the DNS registry for the domain name, a cryptographic asymmetric proof key pair comprising a public key and a private key; providing, by the DNS registry, the public key and a computer executable registry signature verification program for addition to a block in a blockchain of the blockchain network, wherein the registry signature verification program is configured to use the public key to validate signatures made using the private key; receiving, by the DNS registry, a request for a proof of registrar of record for the domain name from a registrar of record for the domain name, wherein the request comprises the domain name; confirming, by the DNS registry, that the registrar is a registrar of record for the domain name; providing, by the DNS registry, a proof of registration message, wherein the proof of registration message comprises a signature by the private key and confirms that the registrar is a registrar of record for the domain name; whereby the registry signature verification program validates the signature using the public key, and whereby the blockchain network receives and stores in the blockchain an association between the domain name and an existing blockchain user address for the registrant.

Various optional features of the above method embodiments include the following. The method may further include: using the private key, signing, by the DNS registry, a top level domain name corresponding to the domain name and a blockchain address of the registry signature verification program to form a message; and providing the message to the blockchain network for inclusion in the blockchain. The providing, by the DNS registry, the proof of registration message may include providing, by the DNS registry, the domain name, the existing blockchain user address for the registrant, and the proof of registration message to the blockchain network for processing by the registry signature verification program. The request may further include the